ICS 35.40
L 80

中华人民共和国国家标准

GB/T 22186—2008

信息安全技术
具有中央处理器的集成电路(IC)卡芯片安全技术要求(评估保证级4增强级)

Information security techniques—
Security technical requirements for IC card chip with CPU(EAL4+)

2008-07-16 发布　　2008-12-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准的附录A是规范性附录。

本标准由全国信息安全标准化技术委员会提出并归口。

本标准主要起草单位：中国信息安全产品测评认证中心。

本标准主要起草人：李守鹏、付敏、杨永生、郭颖、潘莹、高金萍、李蒙、祁斌、闫石、胡兵、李刚、陈冈、许珊琳、郑晓光。

引　言

IC卡芯片应用范围的扩大和应用环境复杂性的增加，要求IC卡芯片具有更强的保护数据能力。

本标准在GB/T 18336—2001中规定的EAL4级安全保证要求组件基础上，增加了模块化组件(ADV_INT)，并且将脆弱性分析要求由可以抵御低等攻击潜力的攻击者发起的攻击(组件AVA_VLA.2)提升到可以抵御中等攻击潜力的攻击者发起的攻击(组件AVA_VLA.3)。

本标准仅给出了IC卡芯片应满足的安全技术要求，对IC卡芯片的具体技术实现方式、方法等不作规定。

信息安全技术
具有中央处理器的集成电路(IC)卡芯片
安全技术要求(评估保证级4增强级)

1 范围

本标准规定了对具有中央处理器的集成电路(IC)卡芯片达到EAL4增强级所要求的安全功能要求及安全保证要求。

本标准适用于IC卡芯片的研制、开发、测试、评估和产品的采购。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准,然而,鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本标准。

GB/T 18336.1—2001 信息技术 安全技术 信息技术安全性评估准则 第1部分:简介和一般模型(idt ISO/IEC 15408-1:1999)

GB/T 18336.2—2001 信息技术 安全技术 信息技术安全性评估准则 第2部分:安全功能要求(idt ISO/IEC 15408-2:1999)

GB/T 18336.3—2001 信息技术 安全技术 信息技术安全性评估准则 第3部分:安全保证要求(idt ISO/IEC 15408-3:1999)

3 术语、定义和缩略语

GB/T 18336—2001确立的以及下列术语、定义和缩略语适用于本标准。

3.1 术语和定义

3.1.1

智能卡 smart card

具有中央处理器(CPU)的集成电路卡,即IC卡,是将一个具有中央处理器的集成电路芯片镶嵌于塑料基片中,并封装成卡的形式。从数据传输方式上可分为接触式IC卡和非接触式IC卡。

3.1.2

IC专用软件 IC dedicated software

由IC卡芯片设计者开发并且在集成电路生产者交付之后依然以物理形式存在于智能卡集成电路中的专用软件。这些专用软件通常在生产过程中用于测试,也可以用来提供额外的服务以便于硬件的使用或提供附加的服务。

3.1.3

初始化数据 initialization data

在IC卡芯片制造阶段写入的与制造有关的数据,如IC卡芯片的标识号。

3.1.4

个人化数据 personalization data

在个人化阶段写入的数据。